Electronic Letters on Computer Vision and Image Analysis 6(1):1-12, 2007

A colour Code Algorithm for Signature Recognition

Vinayak Balkrishana Kulkarni

Department of Electronics Engineering. Finolex Academy of Management & Technology, P-60/P-61, Mirjole Block MIDC,Ratnagiri, Maharashtra. INDIA- 415639

Received 29 November 2005; Accepted 16 January 2007

ABSTRACT

The paper "A Colour Code Algorithm for Signature Recognition" accounts an image processing application where any user can verify signature instantly. The system deals with a Colour code algorithm, which is used to recognize the signature.

The paper deals with the recognition of the signature, as human operator generally make the work of signature recognition. Hence the algorithm simulates human behavior, to achieve perfection and skill through AI. The logic that decides the extent of validity of the signature must implement Artificial Intelligence Pattern recognition is the science that concerns the description or classification of measurements, usually based on underlying model. Since most pattern recognition tasks are first done by humans and automated later, the most fruitful source of features has been to asked the people who classify the objects how they tell them a part . Signatures are a behavioural biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name

The algorithm is tested on various operating systems & we find that it works very well & satisfactory. While implementing the recognition process, we have used quite simpler way. At this stage we are getting accuracy up to about 80% to 90%.

Key words: Pattern Recogniton, Signature Reognition, Image Morphology, Colour Code Algorithm.

1. INTRODUCTION

Pattern recognition is the science that concerns the description or classification of measurements, usually based on underlying model. Since most pattern recognition tasks are first done by humans and automated later, the most fruitful source of features has been to asked the people who classify the objects how they tell them a part. Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples

Correspondence to: <vinay2919702@gmail.com>
Recommended for acceptance by <E. Marti>
ELCVIA ISSN: 1577-5097
Published by Computer Vision Center / Universitat Autonoma de Barcelona, Barcelona, Spain

for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioural biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name [1], [2]

2.0 BIOMETRIC AUTHENTICATION & SIGNATURE VERIFICATION

2.1 INTRODUCTION

Automatically verifying someone's identity by his face, iris or fingerprint is no longer science fiction, but rather it became a daily routine authentication procedure in many places. Biometrics is the utilization of physiological Characteristics (face, iris, and fingerprint) or behavioural traits (signature, voice) for identity verification of an individual, though the complete list of characteristics is much longer. Biometric authentication is gaining popularity as a more trustable alternative to password-based security systems, since it is almost impossible to steal, copy, or guess biometric properties. Furthermore, one can forget his password, whereas forgetting is even not an issue for biometric properties. While looking for a proper biometric to be used in a particular application, following criteria are important: i) uniqueness, ii) whether it is hard to be copied or stolen, iii) acceptability by the public, iv) and the cost to employ that particular biometric data. [3], [4]

Signature is a behavioural biometric: it is not based on physiological properties of the individual, such as fingerprint or face, but behavioural ones. As such, one's signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public, make it more suitable for certain lower-security authentication needs. For instance, MasterCard estimates a $450 million loss each year due to credit card fraud, likewise some billions of dollars being lost because of fraudulent encashment of checks. Reliable automatic signature verification could be a proper solution to reduce such losses since handwritten signatures are already involved in the credit card transactions and bank checks encashment. On-line signatures are more unique and difficult to forge than their counterparts are, since in addition to the shape information, dynamic features like speed, pressure, and capture time of each point on the signature trajectory are available to be involved in the classification. In other words, on-line signatures have an extra dimension, which is not available for the off-line signatures. As a result, on-line signature verification is more reliable than the off-line. Figure summarizes the task to be solved by a signature verification system: given a test signature and a claimed ID, either accept a user as the identity owner or deny him based on a dissimilarity degree between the test and reference set signatures. In either of the signature verification systems, the users are first enrolled by providing reference signature samples. When a user presents a test signature and claims to be a particular individual, the test signature is compared with reference set signatures of the claimed identity. If the dissimilarity between the test and reference set signatures is above a certain threshold, the user is rejected, otherwise accepted. [3], [5]

The dissimilarity between two signatures can be established in two ways: if each time a signature is presented to the system, equal number of features is being extracted from that signature, some sort of distance (ex. Euclidian distance) can be used to compare these two signatures. In this type of comparison, global features which describe the signature as a whole are used. Systems using only global features are generally fast but have low performance. The second alternative is to make a point-by-point comparison, where the so called local features, pertaining to particular points on the signature trajectory, are used. Since even signatures signed by the same person may vary in length (implying feature vectors of different length), methods which are able to non-linearly associate vectors of different lengths, such as Dynamic Time Warping (DTW) or Hidden Markov Models (HMM) are used. Since obtaining actual forgeries is difficult, two forgery types have been defined: A skilled forgery is signed by a person who has had access to a genuine signature for practice. A random or zero-effort forgery is signed without having any information about the signature, or even the name, of the person whose signature is forged. State of the art performance of the available on-line signature verification algorithms lies between 1% and 10% equal error rate, while off-line verification performance is still between 70% and 80% equal error rate. Unfortunately no public signature database of either type is available, which makes it difficult to compare existing signature verification systems. [6], [5], [11]

2.2 ON-LINE SIGNATURE VERIFICATION

Nalwa in his work [17] claims that the behavioural characteristics of a signature are not as consistent as its shape information. He summarizes his algorithm in three phases: normalization, description, and comparison. Normalization was used to make the algorithm invariant to changes in signature's orientation (rotation) and aspect ratio (size). First a polygon was fitted through the sample points of signature trajectory. Then signature was normalized with respect to rotation and aspect ratio of fitted polygon. The jitter, the aspect ratio and number of strokes were extracted prior to the normalization, and kept as global features. During the description phase, five characteristic functions were derived, each describing a local feature of the signature. Features described are: the x and y coordinates relative to the center of mass, the torque and two curvature-ellipses measures derived from the moments of inertia. Each function then was normalized to have zero mean. Finally, comparison was providing the dissimilarity measure between the signature and a claimed prototype. To do so, characteristic functions were simultaneously warped against their prototypes, resulted in the overall alignment cost. The alignment cost was then considered as a global feature. The final dissimilarity measure was defined as the weighted harmonic mean of the global features. The system was tested using three different data sets of 904, 982 and 790 genuine signatures, where 59, 102 and 43 writers contributed to, respectively. Additionally, 325, 401 and 424 forgery signatures were collected. Using 6 reference signatures for the prototype creation, Nalwa reported equal error rates of 3%, 2% and 5%, for each data set respectively. [17]

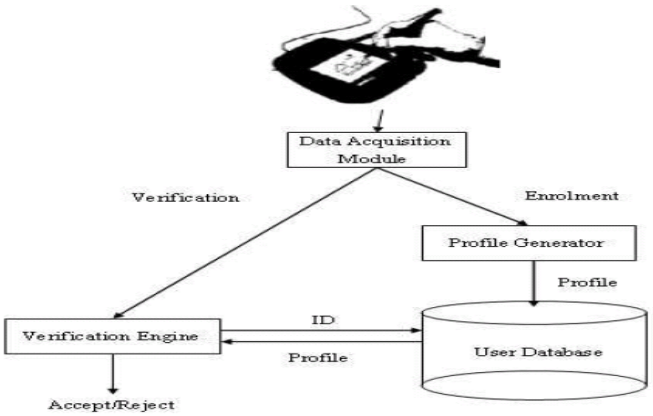

Fig 1.0 On-line signature Verification System

2.3 OFF-LINE SIGNATURE VERIFICATION

Literature Overview Automatic off-line signature verification is a very old pattern classification problem, involving the discrimination of genuine and forgery signatures, written on a piece of paper. Unlike on-line systems, off-line systems have only the image of a signature as input; in other words, dynamic information is not available for the off-line signature verification. Other difficulties such as variation within genuine signatures, noise introduced by the scanning device or a difference in pen width make off-line signature verification a challenging problem. It is worth to notice that, even professional forensic examiners perform at about 70% of correct classification rate (genuine or forgery). The difficulty of the classification can be appreciated by looking at the Figure which depicts four genuine and test signatures. Although the test signature seems to be authentic, it is actually a forgery. [5], [8], [9] [10] *et al*.

3.0 SIGNATURE RECOGNITION USING COLOR CODE ALGORITHM

The paper deals with the recognition of the signature. As human operator generally make the work of signature recognition. Hence the software simulates human behaviour, to achieve perfection and skill through AI. The logic that decides the extent of validity of the signature must implement Artificial Intelligence [15], [16].

The system follows various image processing techniques. The concepts of image morphology such as Thinning, Normalization, and Dilation etc. are implemented. This mainly deal with signature recognition software the system follows the following steps: [1], [13]

- Firstly the signature to be recognized is opened (imported).
- The operations such as normalization, thinning, scaling are performed.
- The standard signature in the database is opened.
- The angle of rotation of the test signature is calculated.
- If required, the test signature is rotated by the difference angle, to compensate the angle change.
- The centroids for both the images are found.
- The check pattern is generated for the standard image.
- According to the centroids the test image is moved and then put on the check pattern.
- The Exclusive-Or operation is performed.
- The resultant pattern is analyzed and the matching percentage is calculated.

Then according to the pattern obtained after the above operation, the intelligent software gives the result using "Colour code algorithm." According to the decision thresholds the decision is given about the validity of the signature.

4.0 COMPARISON WITH OTHER TECHNIQUES

Pattern recognition is the science that concerns the description or classification of measurements, usually based on underlying model. The measurement or the properties used to classify the objects are called as 'features', and the types or categories into which they are classified are called as classes. The two main approaches to pattern recognition are the statistical (decision theoretic) and the syntactic approaches. [17]

We have developed system of colour code algorithm for banking applications. Wherein as per standard baking norms three specimen signatures are taken and while transactions the signature is compared with these specimen signatures. The technique is suitable for both online and offline verification systems. It can be operated in manual or in automated mode. We can primarily classify this technique as Morphological and statistical technique, as no. of matched pixels we categorising and applying different mathematical tools like Autocorrelation. In feature based techniques we have to find different features of each user signature and it is quite difficult and time consuming in case of individual handwriting or signatures on the contrary our technique using pixel by pixel matching it is more accurate and faster than other systems. In case of Syntactic approach pre defined syntax or rules will be different for each specimen. In our technique we are providing preferences to user which indicates how strict verification is required. Wherein our system can achieve 100% accuracy even a single additional dot can be recognised and fake signature can be filtered out (As shown in results). But depending on practical situations and user requirement we can set preferences for accuracy. [14], [5], [6]

While comparing our system with the other techniques in Statistical class like Moment based approach or combination feature and moments or the techniques using Euclidian distance, the accuracy achieved is definitely higher in our system.[9],[10]

5.0 COLOUR CODE ALGORITHM

We are recognizing signature by morphological approach. Here Dilation method is used repetitively to obtain the "Check pattern. This check pattern is obtained from the standard signature will be used for recognition of the signature. The program generates the check pattern, takes the decisions about the validity

of the signature depending the values set In the preferences. The values can be edited by observing the program performance and depending on the application. In the preferences we have different values for the radii for generating the check pattern, the threshold value for the Intensity Normalization operation, the decision Thresholds, the threshold for maximum pixel change, the threshold for maximum rotation angle. Change in any of the above values changes the decision criteria of the program.

5.1 OVERLAPPING AND FINDING THE PERCENTAGE MATCHING:

The important step in the recognition process is the overlapping of the two signatures. The standard signature is opened in a picture box and the check pattern is generated for that image. Then the test signature is processed and the angle of rotations is found, then if there is remarkable change in the angle of rotation, the test signature is rotated through the difference angle. Then the two images are overlapped to generate the final check pattern. The final check pattern is then analyzed as discussed above to find the percentage matching

5.2 PREFERENCES & PERFORMANCE OF THE ALGORITHM:

5.2.1 Setting preferences:

Whenever a new account is being prepared, while storing the signatures in the database and creating the database parameters the program asks the user to select the tolerance option. Three tolerance options are provided by the program, they are

- Global preference
- Exclusively set preference
- Autocorrelation preference.

5.2.1.1 Global preference level:

This preference level includes the standards that are decided by the programmer. These values are found out by experimenting and considering different cases. These values are as follows

- Black band Radius: 16
- Red band Radius: 10
- Green band Radius: 6
- Blue band Radius: 3
- Intensity threshold value: 200
- Maximum pixel change in percentage: 30
- Maximum permissible angle for rotation: 8 Degrees.

DECISION THRESHOLDS:

- Perfect Grade: 95 %
- Better Grade: 90 %
- Good Grade: 82%
- Acceptable Grade: 74 %
- Okay Grade: 64 %

5.2.1.2 Exclusively Set Preferences:

These preferences are set manually by the authorized person. This is because the supervisor may want to give a special importance to a certain customer account. This threshold has to be set exclusively. The

decision thresholds can be set for hard decision or normal decision level. Setting of these preferences drastically affects the performance of the program as well as the decision power. Unless and until one has proper Knowledge about these preferences, one should not try to mess with these values.

5.2.1.3 Autocorrelation preference Level:

Another option for setting the preferences is the autocorrelation preference level. The three standard signatures from the customer are taken as input by the autocorrelation routine. This routine correlates the three signatures with each other and finds out the maximum and minimum matching between the three signatures and decides how much variation is there in the three signature samples.

Depending on these the decision thresholds are set by the program automatically. In case of normal accounts one can set the account to the autocorrelation level. This aspect considers the mutual variation in the three standard signatures, and keeping this variation in mind it decides the signature under test is valid or not. This is a sort of artificial intelligence. The other values are same as the global preference values.

- Black band Radius: 16
- Red band Radius: 10
- Green band Radius: 6
- Blue band Radius: 3
- Intensity threshold value: 200
- Maximum pixel change in percentage: 30
- Maximum permissible angle for rotation: 8 Degrees.

5.2.2 Deviation:

The program finds the percentage matching for a specific signature by calculating the number of pixels lying in the deviation bands in the check pattern. Each band in the check pattern represents a deviation percentage. For example the black band indicates the perfect pixels. The red, Green and blue band indicate 10, 20, 30 percent deviation respectively. The pixels lying in the background colour are having deviation greater than 30 percent. For each pixel having a specific colour, in the check pattern after overlapping the signature, certain marks are assigned, and depending on these marks the percentage matching is found out. The marking scheme is as follows:

- Black pixels 10 (0 -10% Deviation)
- Red pixels 08 (10 -20% Deviation)
- Green pixels 06 (20 -30% Deviation)
- Blue pixels 02 (30 -40% Deviation)
- Background pixels -15 (40-100%Deviation)
- Missing or Extra pixels -18 (Surplus or extra)

These values are calculated from the experimental results and they do not have any firm mathematical base, but they indicate the deviation percentage

6.0 RESULTS

- 1. The signature which is under test is shown below this signature is Colour normalized, scaled, smoothened & then thinned. These operations are illustrated in following figures. The colour normalized signature is then scaled by the required amount as follows

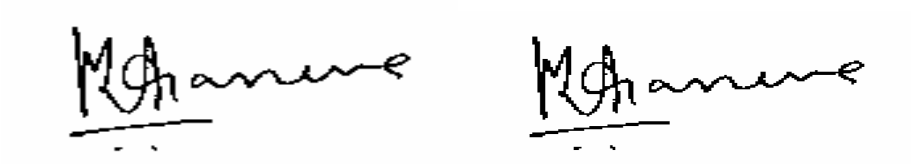

Fig 2.0 Images after Colour Normalization & Scaling

- 2. The scaled signature is then smoothened by applying the smoothening filter, this operation is illustrated below after this, Colour normalization is again performed as follows so as to minimize the loss. This Colour normalized image is thinned as follows.

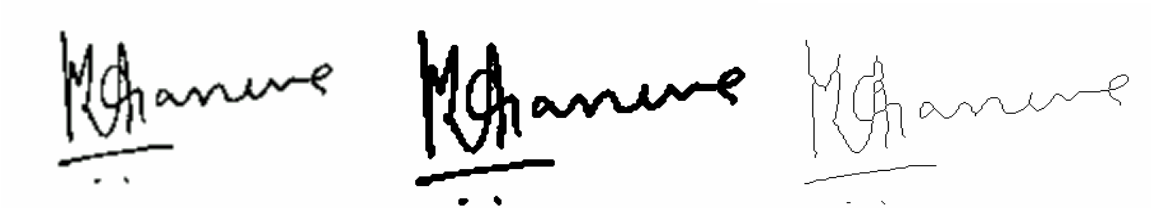

Fig 3.0 Images after Smoothening & thinning

- 3. Then the check-pattern is generated from first standard signature the check-pattern is generated internally by the program after putting test signature on the standard signature as described above looks like following image

Fig 4.0 Check Patterns Generated

- 4. The result of the recognition process is displayed on the panel as follows

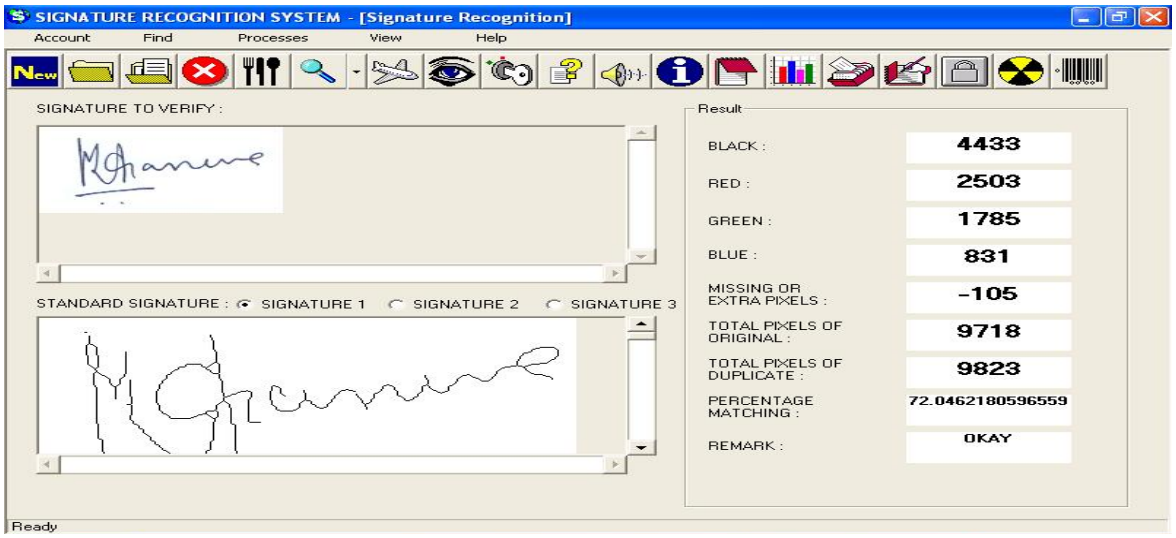

Fig 5.0 Recognition Process

- 5 The report in the html format has following appearance

Tested Area	Results
BLACK PIXELS	4507
RED PIXELS	2564
GREEN PIXELS	1724
BLUE PIXELS	777
MISSING OR EXTRA PIXELS	-120
TOTAL NO. OF PIXELS OF ORIGINAL SIGN	9715
TOTAL NO. OF PIXELS OF DUPLICATE SIGN	9835
PERCENTAGE MATCHING	72.5724453482461%

Fig 6.0 Html report generated

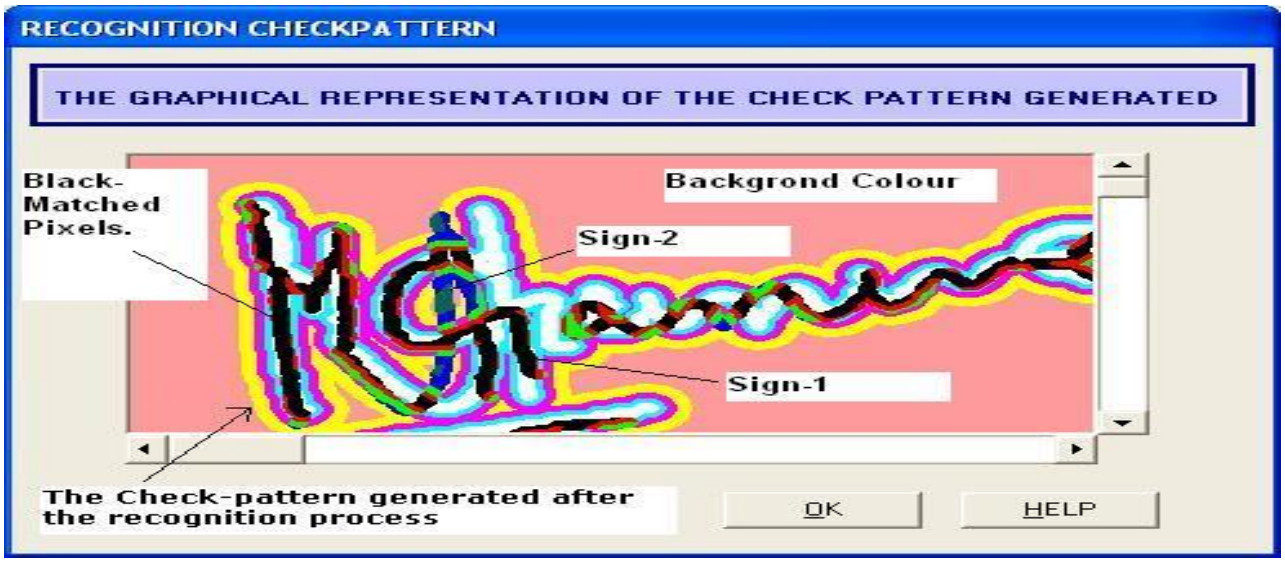

Fig. 7.0 Process of Generation of Check Pattern (Colour Code Algorithm)

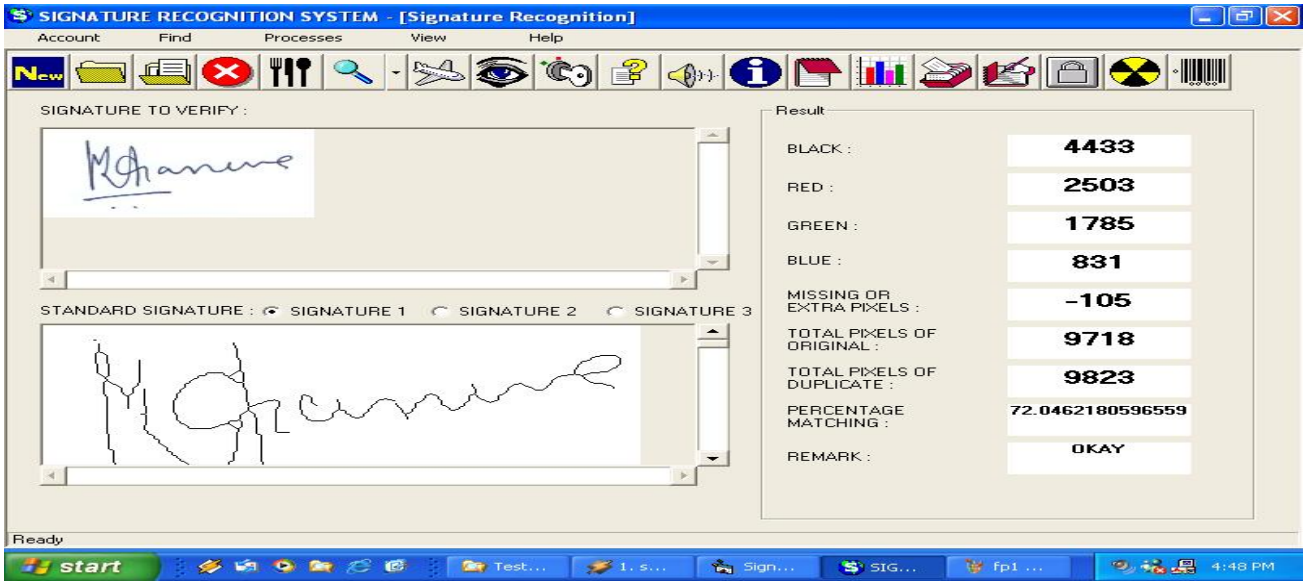

Fig. 8.0 Final Result

- 6. On the same lines we have following four test signatures, the result of recognition process is listed in the table below. The test reports follow on next page.

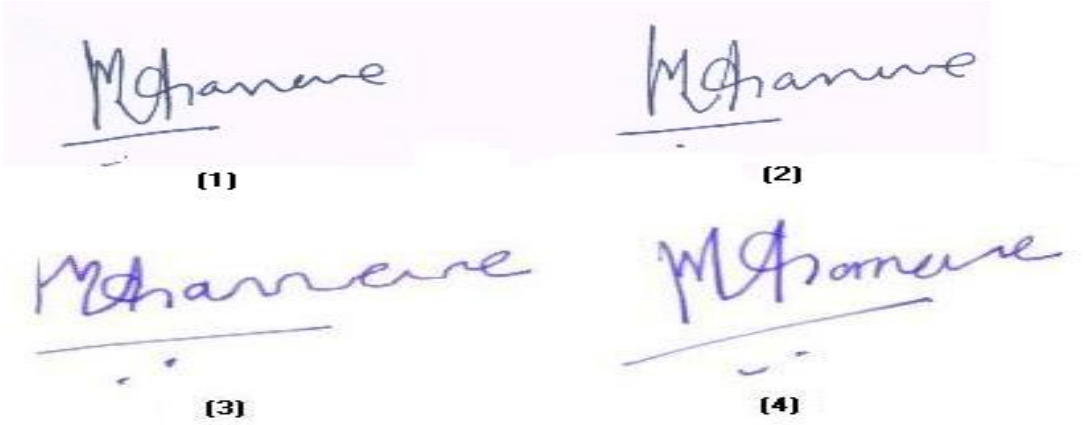

Fig 9.0 Test Signatures with variation

Tested Area	Results
BLACK PIXELS	3093
RED PIXELS	2105
GREEN PIXELS	1714
BLUE PIXELS	1502
MISSING OR EXTRA PIXELS	-778
TOTAL NO. OF PIXELS OF ORIGINAL SIGN	8573
TOTAL NO. OF PIXELS OF DUPLICATE SIGN	9351
PERCENTAGE MATCHING	35.2892738744519%

Fig 10.0 Report generated by the software after checking sign4

PIXELS /SIGNATURES	SIGN 1	SIGN 2	SIGN 3	SIGN 4
BLACK	3806	4509	__	3093
RED	2740	2862	__	2105
GREEN	1984	1811	__	1714
BLUE	722	597	__	1502
MISSING OR EXTRA PIXELS	325	-106	__	-778
PIXELS (ORIGINAL)	9715	9715	__	8573
PIXELS (DUPLICATE)	9390	9821	__	9351
MATCHING (%)	69.66	78.92	__	35.28
REMARKS	Acceptable	Okay	Rejected	Rejected

Fig 11.0 The table summarizing the above operations & the results.

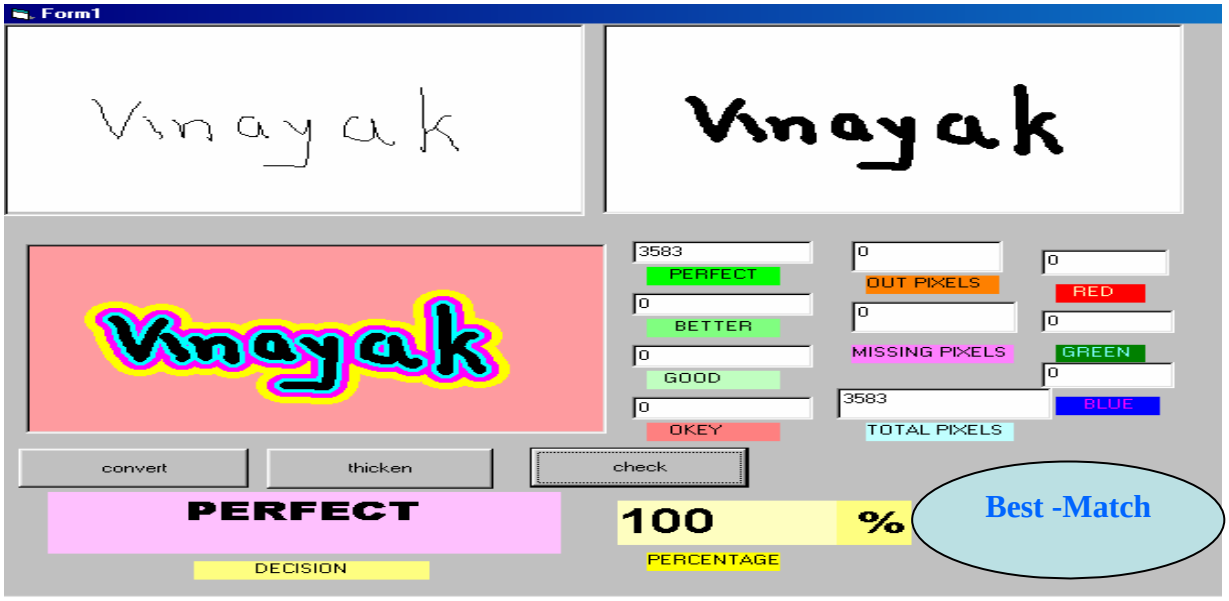

Fig 12.0 The result showing 100 % matching with the specimen signature.

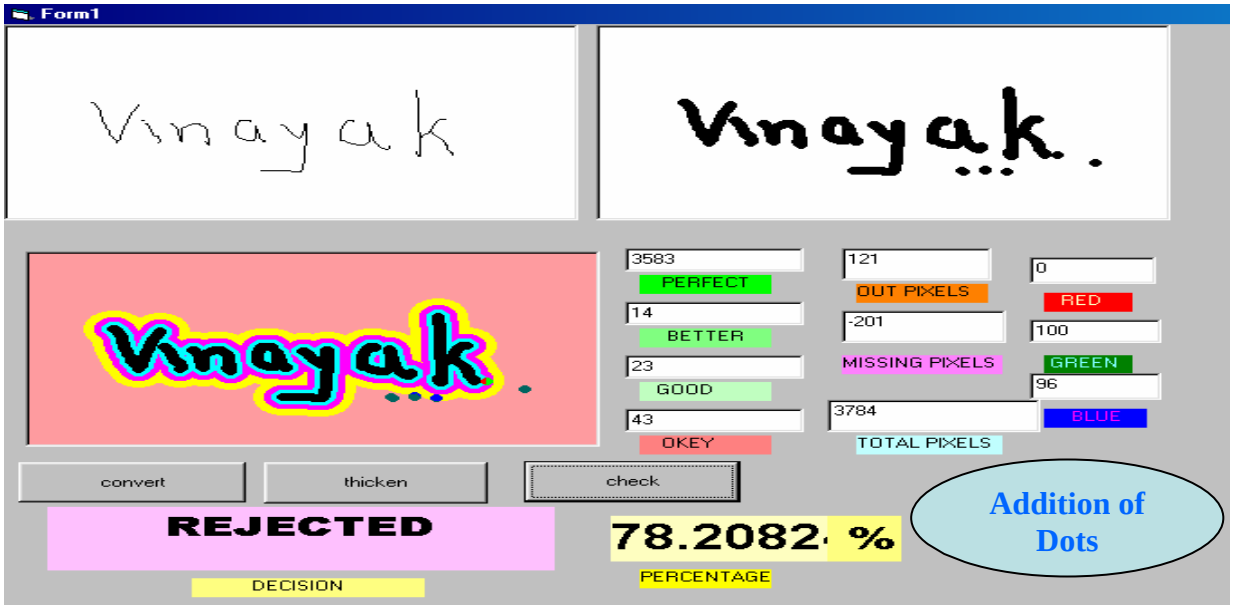

Fig 13.0 The result showing rejection when Dots are added in the specimen signature.

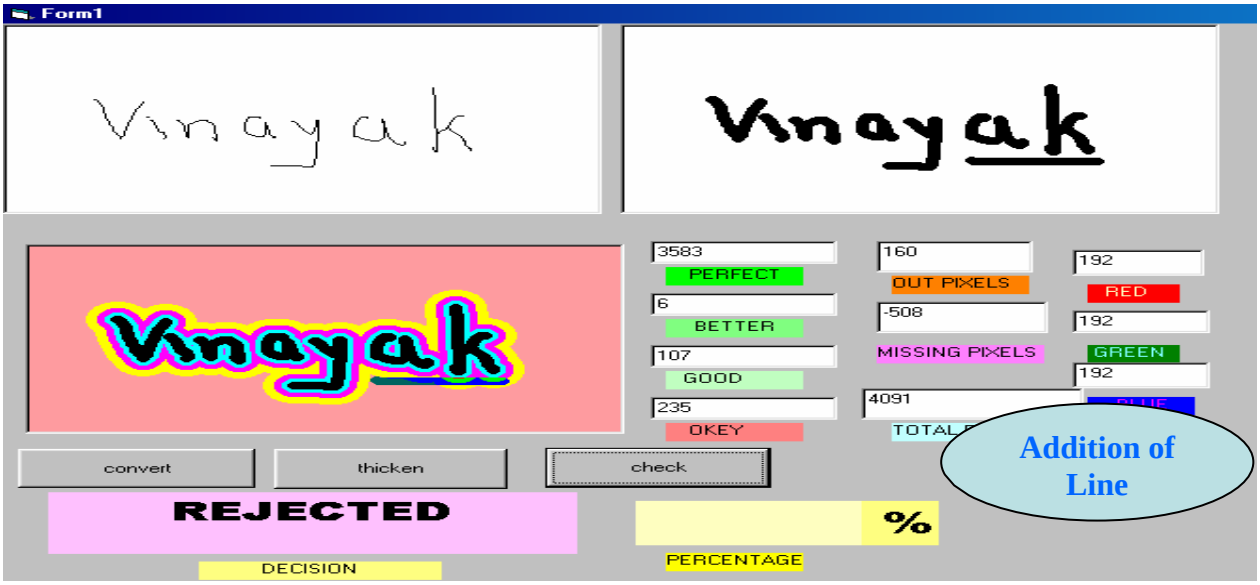

Fig 14.0 The result showing rejection when Line is added in the specimen signature.

Fig 15.0 The result showing rejection for Grade -1 minor variation.

7. SUMMARY AND DISCUSSION

We have tested the software on various operating systems & we find that it works very well & satisfactory. While implementing the recognition process, we have used quite simpler way. At this stage we are getting accuracy up to about 80% to 90%. The accuracy can be achieved up to 100% by implement very tight preferences, but in practical situations tradeoffs can be achieved by user's discretion. After checking several signatures, we found that the irrelevant signatures are surely rejected by the software but it is possible that the signature that one thinks to be passed will be rejected. We have implemented tight preferences for this.

While setting preferences we observed that a definite fuzziness lies in user preferences. In future the system can be configured using Neural Networks and Fuzzy Rule base, where online training of recognition is possible. If system is trained for large database highest accuracy can be achieved.

8. REFERENCES

[1] Milan Sonka, Vaclav Hlavac, Roger Boyle, "Image Processing Analysis, And Machine Vision", Thomson Learning, Singapore, PP 563-64,573,583,593.2002

[2] S Loncaric, A.P. Dhawan," A morphological signature transform for Shape Description." Pattern Recognition, 6:1029-1037. 1993

[3] Kresimir Delac , Mislav Grgic "A survey of biometric recognition methods " ,46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia

[4] B. M. Herbst and H. Coetzer, "On an Off-line Signature Verification System", Proceedings of the 9th annual South African Workshop on Pattern Recognition, pp.39-43, 1998.

[5] Evett and R. N. Totty, "Study Of The Variation In The Dimensions Of Genuine Signatures", Journal of the Forensic Science Society, vol. 25, pp. 207-215, 1985

[6] M. Golfarelli, D. Maio, D. Maltoni, "On the error-reject trade off in biometric Verification Systems," IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 19, pp. 786-796, July 1997

[7] V. S. Nalwa," Automatic On-Line Signature Verification", Proceedings of IEEE, Vol. 85, pp.215-239 , 1997.

[8] B. Fang, C. H. Leung, Y. Y. Tang, K. W. Tse, P. C. K. Kwok, Y. K. Wong, "Off-Line Signature Verification by the Tracking of Feature and Stroke Positions", Pattern Recognition, Vol. 36, pp. 91-101, 2003

[9] Y. Mizukami, H. Miike, M. Yoshimura, and I. Yoshimura, "An Off-Line Signature Verification System Using an Extracted Displacement Function", In Proceedings of ICDAR, pp. 757-760, 1999

[10] W. F. Nemcek and W. C. Lin, "Experimental Investigation of Automatic Signature Verification" IEEE Transactions on Systems, Man and Cybernetics, Vol. 4 , pp. 121-126, 1974.

[11] B. Herbst, D. Richards," On an Automated Signature Verification System", In Proceedings Of IEEE International Symposium of Industrial Electronics , pp. 600-604, 1998.

[12] Anil K. Jain, 'Fundamentals of Digital Image Processing. 'Prentice Hall of India, pp 62, 421.2003

[13] D. Dattaa Majumdar, B.Chanda, "Digital Image Processing and Analysis", New Delhi, Prentice Hall of India , Pp 335, 338,347, 2003.

[14] R M Haralick, S R Stenberg, and X. Zhuang., "Image Analysis Using mathematical Morphology", IEEE Transactions on pattern Analysis and Machine Intelligence, 9(4):532-550. 1987

[15] Nick Efford, "Digital Image Processing" Addison Wesley Longman, Singapore, PP 271, 276,278.2002

[16] Earl Gose, Richard Johnson Baugh, Steve Jost, Rafel, "Pattern Recognition & Image Analysis", Prentice Hall of India.2001

[17] D H Ballard, C M Brown, "Computer Vision", Prentice Hall, Eaglewood Cliffs, NJ USA .1982